REMARKS

In response to the Notice of Non-Compliant Amendment of July 20, 2009, please enter this re-submission of the Amendment originally filed on April 27, 2009.

Claims 1 to 42 were pending in the Application at the time of examination. The Examiner rejected Claims 11, 22 and 33 under 35 U.S.C. 112 for including the term JXTA. The Examiner rejected Claims 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 40, 41, and 42 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1). The Examiner rejected Claims 5, 11, 16, 22, 27 and 33 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1) and further in view of the Rutherglen et al. reference (US2003/0033517A1).

Applicants have cancelled Claims 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 39, and 42 without prejudice.

Applicants have amended Claims 1, 5, 6, 12, 16, 17, 34, 35, 36, 37, 38, 40, and 41. Consequently, Claims 1 to 22, 34, 35, 36, 37, 38, 40, and 41 remain in the Application.

REQUEST FOR EXAMINER INTERVIEW

Should the Examiner be of the opinion that this response does not place the Application in a condition for allowance, Applicants request the Examiner grant an Examiner interview prior to issuance of the next communication from the USPTO. Applicants' Attorney can be reached at (831) 642-9980.

REJECTION OF CLAIMS 11, 22 AND 33 UNDER 35 U.S.C. 112

The Examiner rejected Claims 11, 22 and 33 under 35 U.S.C. 112 for including the term JXTA.

Applicants respectfully submit that the JXTA is an architecture well known in the art. The name is short for Juxtapose, as in side by side, but is not an acronym or proper abbreviation, or simply a trademark. This fact can be established by checking the website at Wikipedia, http://en.wikipedia.org/wiki/JXTA, which reads as follows, with emphasis added:

JXTA (**Juxtapose**) is an open source peer-to-peer protocol specification begun by Sun Microsystems in 2001. Sun remains actively involved in the development and promotion of JXTA. The JXTA protocols are defined as a set of XML messages which allow any device connected to a network to exchange messages and collaborate independently of the underlying network topology. JXTA is the most mature general purpose P2P framework currently available and was designed to allow a wide range of devices - PCs, mainframes, cell phones, PDAs - to communicate in a decentralized manner.

As JXTA is based upon a set of open XML protocols, it can be implemented in any modern computer language. Implementations are currently available for Java Platform, Standard Edition, C/C++/C# and J2ME. The C# Version uses the C++/C native bindings and is not a complete re-implementation in its own right.

JXTA peers create a virtual overlay network which allows a peer to interact with other peers even when some of the peers and resources are behind firewalls and NATs or use different network transports. In addition, each resource is identified by a unique ID, a 160 bit SHA-1 URN in the Java binding, so that a peer can change its localization address while keeping a constant identification number.

In light of the discussion and text above, Applicants respectfully submit that the term JXTA is well defined and known to those of skill in the art and meets the requirements of 35 U.S.C. 112. Consequently, Applicants respectfully request the Examiner withdraw the rejection of Claims 11, 22 and 33 under 35 U.S.C. 112.

REJECTION OF CLAIMS 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36 37, 38, 39, 40, 41, AND 42 UNDER 35 U.S.C. 103(a)

The Examiner rejected Claims 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 40, 41, and 42 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1).

Applicants have cancelled Claims 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 39, and 42 without prejudice. Consequently, Applicants respectfully submit the rejection of Claims 23, 24, 25, 26, 28, 29, 30, 31, 32, 39, and 42 is now moot.

Applicants have amended Claims 1, 5, 6, 12, 16, 17, 34, 35, 36, 37, 38, 40 and 41.

Applicants' independent Claim 1, as amended, reads as follows, with emphasis added:

> A method for securing a communication between a peer node and **a super peer node** in a peer-to-peer network, the method comprising:

the peer node generating a secured communication request to the <u>super peer node, **the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible;**</u>

the **super peer node** authenticating the peer node in response to said secured communication request, and

the **super peer node** issuing a signed certificate of authority upon successful authentication.

Applicants' independent Claim 12, as amended, reads as follows, with emphasis added:

A method for securing a communication between a peer node and a **super peer node** in a peer-to-peer network, the method comprising:

generating a secured communication request to the **super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible,** the secured communication request being capable of authenticating the peer node in response to said secured communication request, and

receiving a signed certificate of authority upon successful authentication.

Applicants' independent Claim 34, as amended, reads as follows, with emphasis added:

> A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for securing a communication between a peer node and a **super peer** node in a peer-to-peer network, the method including:
>
> the peer node generating a secured communication request to the **super peer** node, **the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible**;
>
> the **super peer** node authenticating the peer node in response to said secured communication request, and
>
> the **super peer** node issuing a signed certificate of authority upon successful authentication.

Applicants' independent Claim 35, as amended, reads as follows, with emphasis added:

> A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:
>
> generating a secured communication request to a **super peer** node, **the super peer node being a peer**

node that serves as an intermediary contact point for
administrative information that concerns the super
peer node as well as a subset of the peer-to-peer
network associated with the super peer node and for
which the super peer node is responsible, the secured
communication request being capable of authenticating
the peer node in response to said secured
communication request, and

receiving a signed certificate of authority upon
successful authentication.

Applicants' independent Claim 36, as amended, reads
as follows, with emphasis added:

A program storage device readable by a machine,
tangibly embodying a program of instructions
executable by the machine to perform a method for
administrating peer-to-peer networks, the method
including:

a super peer node receiving a secured
communication request from a peer node, the super
peer node being a peer node that serves as an
intermediary contact point for administrative
information that concerns the super peer node as well
as a subset of the peer-to-peer network associated
with the super peer node and for which the super peer
node is responsible;

authenticating the peer node in response to said
secured communication request; and

sending a signed certificate of authority upon
successful authentication.

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0860
Fax (831) 655-0888

Page 15 of 23

Applicants' independent Claim 37, as amended, reads as follows, with emphasis added:

> An apparatus for securing a communication between a peer node and a **super peer** node in a peer-to-peer network comprising:
>
> means for generating a secured communication request to the **super peer** node, **the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible**;
>
> means for authenticating the peer node in response to said secured communication request, and
>
> means for issuing a signed certificate of authority upon successful authentication.

Applicants' independent Claim 38, as amended, reads as follows, with emphasis added:

> An apparatus for securing a communication between a peer node and a **super peer** node in a peer-to-peer network comprising:
>
> means for generating a secured communication request to the **super peer** node, **the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible, the secured communication request being**

capable of authenticating the peer node in response
to said secured communication request, and
means for receiving a signed certificate of
authority upon successful authentication.

Applicants' independent Claim 40, as amended, reads as
follows, with emphasis added:

A peer-to-peer network system comprising:
a peer node;
a super peer node communicatively coupled to
said peer node**, the super peer node being a peer node
that serves as an intermediary contact point for
administrative information that concerns the super
peer node as well as a subset of the peer-to-peer
network associated with the super peer node and for
which the super peer node is responsible**;
wherein said peer node is configured to
generate a secured communication request to said
super peer node;
wherein said **super peer** node is configured
to authenticate said peer node in response to said
secured communication request, and
wherein said **super peer** node is configured
to issue a signed certificate of authority upon
successful authentication.

Applicants' independent Claim 41, as amended, reads as
follows, with emphasis added:

A peer node comprising:
a processor; and

> a memory comprising program instructions,
> wherein the program instructions are executable by
> the processor to:
>
> > generate a secured communication request to
> > **a super peer** node, **the super peer node being a peer**
> > **node that serves as an intermediary contact point for**
> > **administrative information that concerns the super**
> > **peer node as well as a subset of the peer-to-peer**
> > **network associated with the super peer node and for**
> > **which the super peer node is responsible, the secured**
> > **communication request being** capable of authenticating
> > the peer node in response to said secured
> > communication request, and
> >
> > receive a signed certificate of authority
> > upon successful authentication.

As shown above, each of Applicants' independent Claims, as amended, specifically recites **a super peer** node**, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible**.

In addition, as also shown above, each of Applicants' independent Claims, as amended, specifically recites authentication of a peer node by the **super peer node**.

A "super peer" or "super peer node", is defined in Applicants' Specification at, for example, page 8, paragraph [0014] to page 9, paragraph [0016], which reads as follows, with emphasis added:

> **Super peer nodes are peer nodes that serve as an**
> **intermediary contact point for administrative**

information that concerns the super peer nodes as well as the subset of the P2P network of which they are aware and for which they are responsible. These super peer nodes may be used to respond to Certificate Service Requests from peer nodes.

FIG. 2 is a diagram schematically illustrating intermediary peer nodes mediated P2P connections in accordance with one embodiment of the present invention. To improve peer node discovery, responsiveness of communication, and routing **super-peers** have been introduced into P2P network topologies. A first peer node 202 is connected to a network connection 204, such as the internet, through a first Network Address Translator (NAT) 206. A first super peer node 208 is connected to the network connection 204 through a first JXTA relay 209 and a first router 210. A second super peer node 212 is connected to the network connection 204 through a second JXTA relay 213 and a second router 214. A second peer node 216 is connected to the network connection 204 through a second Network Address Translator (NAT) 218. It must be understood that there may be multiple routers in these network paths as well as firewalls. FIG. 2 is illustrative of one of many means to separate peer nodes and super peers on the Internet.

Super peers, **also known as intermediary peer nodes**, may be added with a minimal amount of centralization, and may be placed in an ad-hoc topology to be discovered by chance, or by an email message containing a known IP address and a port of a super peer. Once the presence of the super peer is known, the knowledge of their existence can be propagated amongst the peer nodes or edge-peers as

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0980
Fax (831) 655-0888

they contact one another. Such super peer 208, 212, may also serve as a contact point for administrative information that concerns the super peers themselves as well as the subset of the P2P network (in FIG. 2, the subset of the P2P network includes peer node 202 and peer node 216) of which they are aware and for which they are responsible.

As shown above, in accordance with Applicants' Specification, a "Super Peer Node" is defined as a node with specific properties, not simply another node on the P2P network.

In addition, at paragraphs [0017] to [0021] of Applicants' Specification, Applicants specifically state, with emphasis added, that:

With respect to the implementation of securing P2P networks, the present invention is described in the context of ad-hoc JXTA P2P networks. The present description is for illustrative purposes and **the method for securing P2P networks is independent of the implementation of the underlying P2P platform <u>as long as this platform adheres to the following minimal characteristics</u>**:

1. **The P2P network topology is organized <u>around super peers</u>** such as super peer node 208 and super peer node 212 in FIG. 2.

2. **The <u>super peer nodes</u> have knowledge of one another, and have the ability to communicate with one another on the P2P network.** In FIG. 2, super peer node 208 is aware of the existence of super peer node 212 and super peer node 208 can communicate with

super peer node 212 via routers 210, 214 and network connection 204.

3. **Each peer node of the P2P network connects to at least one of the super-peers on a regular basis**. For example, peer nodes 202 and 216 connect to super peer node 212 on a regular basis.

One of the primary axioms of P2P networks is end-to-end communication: any two peer nodes must be able to communicate, and either of them must be able to initiate a connection to the other. Because peer nodes 202, 216 are both NAT bound, neither peer nodes 202 and 216 can initiate connections to one another unless a connection is mediated through a common known third party intermediary, such as super peer node 212. In FIG. 2, peer node 202 communicates with peer node 216 via super peer node 212. Discovery or address lookup given a name is therefore handled by the super peers 208 and 212. The same initiation of communication barrier can be affected by a firewall or combinations of NAT and firewalls.

As shown above, in accordance with Applicants' Specification, a super peer node is defined specifically as a node with specific properties, not simply another node on the P2P network, and the intermediary peer nodes, as defined, are required.

Applicants respectfully submit that nowhere in the Vigue reference, the Winget reference, or any proper combination of the Vigue reference and the Winget reference, is **a super peer** node**, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-**

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Page 21 of 23

to-peer network associated with the super peer node and for
which the super peer node is responsible, discussed, disclosed,
taught or suggested.

Consequently, Applicants respectfully request the Examiner
withdraw the rejection of Claims 1, 12, 34, 35, 36, 37, 38, 40,
and 41, as amended, and allow Claims 1, 12, 34, 35, 36, 37, 38,
40, and 41, as amended, to issue.

In addition, Claims 2 to 11, as amended depend, directly
or indirectly, on Claim 1, as amended, and Claims 13 to 22, as
amended, depend, directly or indirectly, on Claim 12, as
amended. Consequently, Applicants respectfully request the
Examiner withdraw the rejection of Claims 2 to 11 and 13 to 22,
and allow Claims 2 to 11, and 13 to 22 to issue as well for at
least the reasons discussed above.

REJECTION OF 5, 11, 16, 22, 27 and 33 UNDER 35 U.S.C. 103(a)

The Examiner rejected Claims 5, 11, 16, and 22 under
35 U.S.C. 103(a) as obvious over the Vigue et al. reference
(US 2003/0163702A1) in view of the Winget et al. reference
(US2005/0120213A1) and further in view of the Rutherglen et al.
reference (US2003/0033517A1).

As noted above, Applicants have cancelled Claims 23, 24,
25, 26, 27, 28, 29, 30, 31, 32, 33, 39, and 42 without
prejudice. Consequently, Applicants respectfully submit the
rejection of Claims 27 and 33 is now moot.

As discussed above, Applicants' independent Claims 1 and
12, as amended, specifically recite a super peer node, the
super peer node being a peer node that serves as an
intermediary contact point for administrative information that
concerns the super peer node as well as a subset of the peer-
to-peer network associated with the super peer node and for
which the super peer node is responsible.

As also discussed above, Applicants respectfully submit
that nowhere in the Vigue reference, the Winget reference, or

GUNNISON, McKAY &
HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0881
Fax (831) 655-0388

any proper combination of the Vigue reference and the Winget reference, is **a super peer** node, **the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible,** discussed, disclosed, taught or suggested.

Applicants further submit that the addition of the Rutherglen reference does nothing to cure this deficiency of the Vigue reference, the Winget reference, or any proper combination of the Vigue reference and the Winget references.

Claims 5 and 11, as amended, depend on Claim 1 as amended. Claims 16 and 22, as amended depend on Claim 23, as amended. Consequently, Applicants respectfully request the Examiner withdraw the rejection of dependent Claims 5, 11, 16, and 22 and allow Claims 5, 11, 16, and 22 to issue for at least the reasons discussed above with respect to parent Claims 1, and 12, as amended.

<div align="center">CONCLUSION</div>

For the foregoing reasons, Applicants respectfully request allowance of all pending Claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicants.

Respectfully submitted,

Philip McKay
Attorney for Applicants
Reg. No. 38,966
Tel.: (831) 655-0880